



CITY OF AKRON, OHIO
POLICE DIVISION
JAMES D. NICE, CHIEF OF POLICE

NUMBER P-2011-026	EFFECTIVE DATE October 31, 2011	RESCINDS P-09-026
SUBJECT Computer Equipment Procedure	ISSUING AUTHORITY Chief James D. Nice	

I. POLICY

Executive Order #10-2005, dated December 1, 2005, issued by the Mayor of the City of Akron, Ohio, on computer, electronic mail, Internet, and intranet usage outlines the City of Akron's policy for computer use. This procedure is to supplement the city's policy and provide additional guidelines.

II. DEFINITIONS

- A. Computer resources – Includes, but not limited to: servers, workstations, stand-alone computers, laptops, printers, scanners, Mobile Data Terminals (MDT's), Mobile Data Browsers (MDB's), Personal Digital Assistants (PDA's), software, data and all internal and external computer and communications networks (for example, Internet, e-mail, LEADS and other jurisdictions or agencies).
- B. Computer data – Information that is being or has been prepared in a formalized manner intended for use in a computer system.
- C. Computer virus – A computer program that copies itself into other programs stored in a computer with either a benign or negative effect.
- D. Hardware – The computer and associated physical equipment directly involved in its presence.
- E. Shareware, freeware, open source – A method of distributing software programs whereby the programmer will allow anyone to use or share his programs for some specified period of time with the expectation that the user will abide by the license which may include payment or registration.
- F. Software – The programs and applications that control the functioning of the computer.

III. PROCEDURE

A. HARDWARE

1. All hardware installed within this department is the property of the Akron Police Department and shall not be moved to any other location without the express authorization of the Information Systems Unit. This includes moving equipment within a particular unit from one location to another. *Network data connections make it*

October 31, 2011

imperative that Information Systems personnel shall be the only ones to move the equipment.

2. Employees are not to perform any maintenance on the hardware with the exception of cleaning or dusting of the exterior cases and cleaning of the monitor screen and keyboard.
3. No personal hardware (modems, cameras, PDA's, speakers, etc.) is to be installed without the approval of the Information Systems Unit.

B. SOFTWARE

1. The Akron Police Department will supply software to be used on department owned computers. No other software from any other source may be installed without the authorization of the Information Systems Unit. This includes, but is not limited to, software personally owned by employees or available in the public domain. Employees shall not remove departmental software applications from the Safety Division computers.
2. Software will be considered for installation by the department for employees who express a need. Such requests for software programs should be made in writing through the chain of command to the Information Systems Unit. If the requested software is approved, the department will acquire, install and keep it in inventory.
3. Employees, except for authorized Information Systems personnel, shall not install software from one computer to another, nor are copies to be made for personal computers, notebooks, etc. without specific authorization from the Information Systems Unit. Software license agreements entered into by the City of Akron with all software providers must be observed.
4. It is the policy of this department to abide by all software copyright agreements and to adhere to the terms of all software licenses to which the City of Akron is a party. Employees who violate any of the policies defined herein may be subject to the appropriate criminal, civil, or departmental disciplinary action. Any employee who determines that there may be a misuse of software within this department shall notify their supervisor or the Information Systems Unit.
5. Current hardware and software technology offers the opportunity for some individuals to customize their workstations by displaying personalized backgrounds, screensavers, or by playing digitized sound. Some of these features could be construed as being offensive, suggestive, sexually oriented, or disruptive to the work environment by others. If there is any question concerning the appropriateness of any computer workstation display or sounds, the issue should be referred to the unit supervisor or the Information Systems supervisor, who will determine the suitability of the material in the work environment.

October 31, 2011

C. COMPUTER DATA

1. Employees should be aware that information on departmental computers could be subject to public records requests. However, some information is exempt from public records law and could violate departmental rules and regulations if disseminated. Public requests for information on a departmental computer should be referred to the Police Information Officer (PIO).
2. Departmental rules and regulations prohibit officers from disseminating information stored on department computers. However, employees may disseminate information to authorized individuals.

D. EXPECTATION OF PRIVACY

1. Computer resources are owned and maintained by the Akron Police Department, which reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of computer resources, with the following exceptions:
 - a. No hardware, software, or digital information that is evidence or contraband; i.e., photos depicting pornography or child pornography, will be viewed, copied, or shared in any way with anyone not directly involved with the investigation and prosecution of the case or supervisors in their direct chain of command.
 - b. Computer resources used to facilitate a criminal investigation will generate information and reports that are part of the case file. No person other than assigned investigators and prosecutors, or supervisors in their direct chain of command, may copy or disseminate in any way any information, digital or otherwise, contained in a case file until that file becomes public record.
 - c. Investigations conducted online may require the use of false identities and role-playing. When done in furtherance of an investigation, this is entirely appropriate and is in no way a violation of the procedure or any city policy or procedure.
2. Users understand that human or automated means may be used to monitor use of computer resources including communications, Internet access, data access, and other content transmitted, received, or stored.

E. SECURITY

1. Users are responsible for safeguarding their passwords and are responsible for all transactions made with their passwords.
2. No user shall allow access to their password or account by another, nor will any user use another's password or account.

F. E-MAIL

1. E-mail accounts are created based on assignments. In the event that a user needs an account, the user should make a request through the chain of command.

October 31, 2011

2. E-mail should never be considered private or secure. It may be stored indefinitely on any number of computers, including that of the recipient. Copies of messages may get forwarded to others. E-mail sent to nonexistent or incorrect user names may be delivered to persons that were never intended to receive it.
3. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate shall not be sent by e-mail.
4. Chain letters are messages sent to a number of people asking each recipient to send copies to a number of other users. They consume resources and can degrade network performance or delay delivery of essential e-mail. Users should immediately delete such e-mail. If a user has received such a message that has a legitimate need to get forwarded, it should first be evaluated for authenticity and approved by a supervisor or by the Information Systems Unit.

G. INTERNET

1. The Internet is a valuable source of information and research. Internet accounts may be provided to certain employees based on assignment to assist them in performing their jobs. In the event that a user needs an account, the user should make a written request through the chain of command.
2. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate shall not be downloaded, copied or forwarded. Exceptions may be granted if the stated material is being used by the employee who is investigating criminal or civil actions.
3. Abuse of Internet privileges shall result in the loss of these privileges. In addition, the employee may be subject to disciplinary action, including possible termination, civil and criminal liabilities.

H. COMPUTER VIRUS PROTECTION

1. The end user is not required to perform any antivirus updates or scans. The updates and scans will be coordinated systematically by Information Systems personnel based on daily, weekly, and monthly needs and requirements.
2. Any employee who suspects that there may be a breach of information, computer hacking, sabotage to software or hardware, or computer virus shall immediately discontinue any further transactions and leave the computer as is.
3. Notify a Safety Communications supervisor immediately.
4. Supervisors shall notify Information Systems immediately according to the Information Systems Unit guidelines.
5. The Information Systems Unit supervisor will complete a LEADS Computer Incident Report Form in the event of a confirmed computer or network incident within our agency.

October 31, 2011

6. Antivirus awareness training will be reviewed biannually.

I. COPYRIGHTS

1. All software licensed by the City of Akron is copyright protected. It is the policy of the City of Akron not to violate copyright laws. Duplicating, selling, or otherwise copying for purposes of distributing software products, other than that which is agreed to under the terms of the software license agreement, is a violation of federal law and is forbidden by the City of Akron. The Federal Copyright Act makes no distinction between duplicating software for sale or for free distribution.
2. The rights of copyright owners will be respected. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. This includes copying text, graphics or photographs. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, it should be assumed that they are protected under copyright laws unless there is explicit permission on the materials and their use.

J. EMPLOYEE ACKNOWLEDGMENT

1. All employees shall read and sign an Employee Acknowledgment for the Safety Computer Network.
2. A copy of the signed Employee Acknowledgment form will become a part of the employee's permanent file, which is maintained in the office of the Chief of Police.

By Order Of,



James D. Nice
Chief of Police

Date October 13, 2011